《信息安全及实践》课程实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 学院： | 信息学院 | 专业： | 计算机科学与技术 | 年级： | 2019 |

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名： | 赵浩杰 | 学号： | 20191060074 |
| 姓名： | 李泽昊 | 学号： | 20191060065 |
| 姓名： | 白文强 | 学号： | 20191060064 |

|  |  |
| --- | --- |
| 实验时间： | 2021年10月29日 |

|  |  |
| --- | --- |
| 实验名称： | 安全端口实验和防DHCP欺骗攻击实验 |

|  |  |
| --- | --- |
| 实验成绩： |  |

安全端口实验

一、实验目的

(1)验证交换机端口安全功能配置过程。

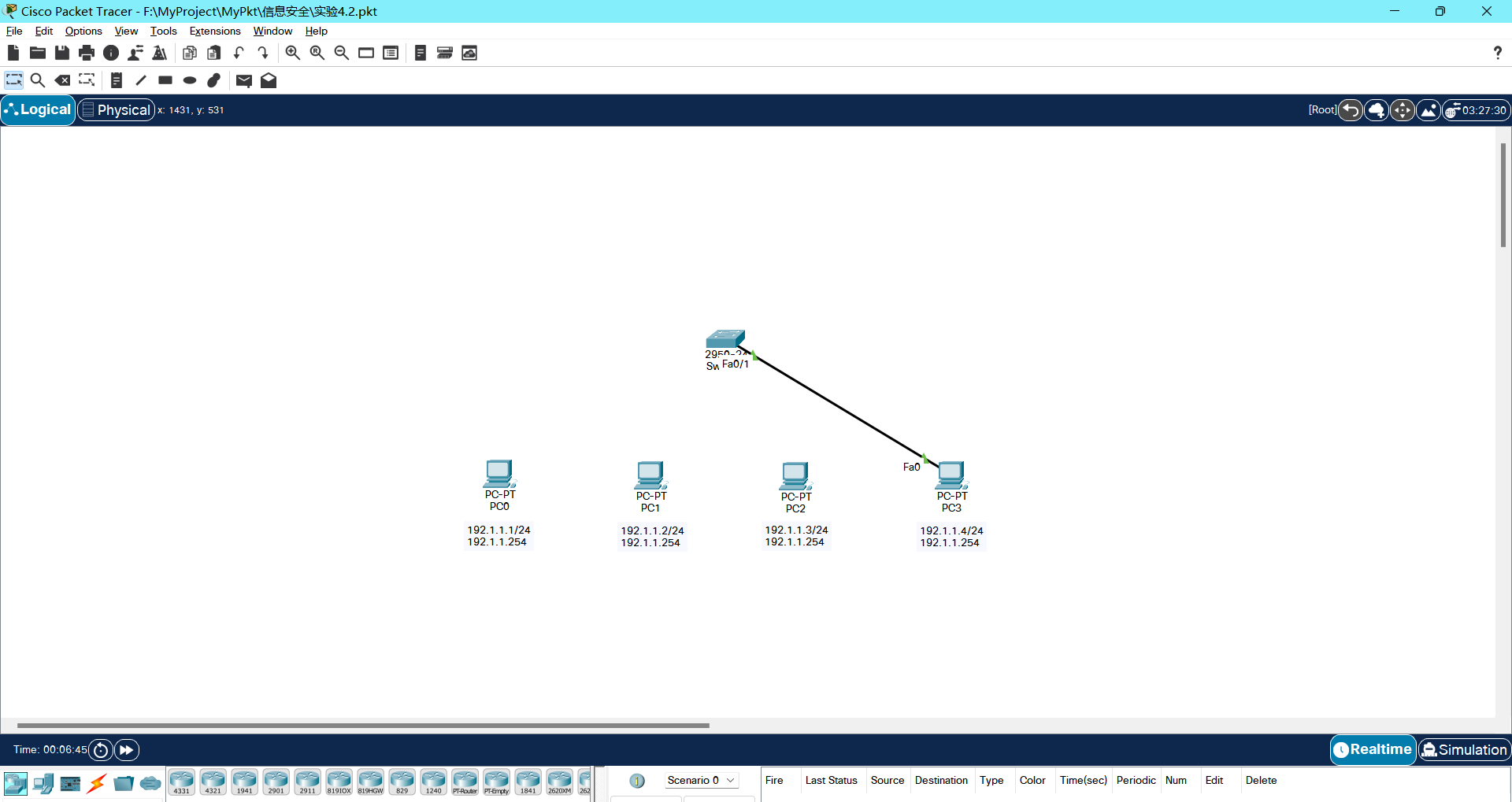
(2)验证访问控制列表自动添加MAC地址的过程。

(3)验证对违规接入终端采取的各种动作的含义。

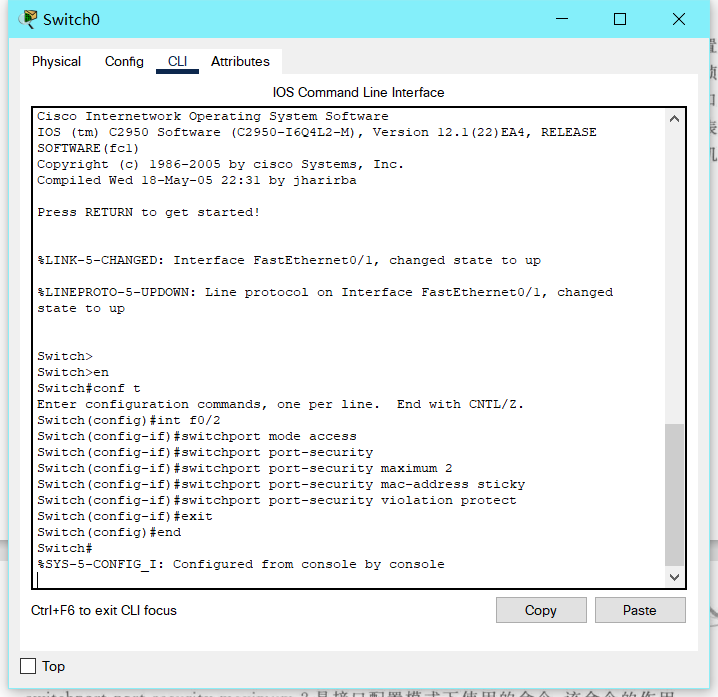
(4)验证安全端口方式下的终端接入控制过程。

二、实验步骤

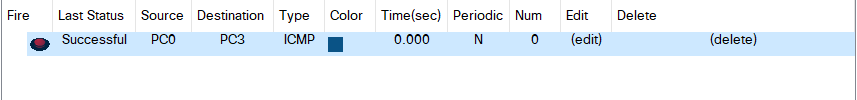
1. 完成4个终端PC0、PC1、PC2和PC3以及交换机的拓扑图,配置好4台终端的网络信息，将PC3连接到交换机端口F0/1；



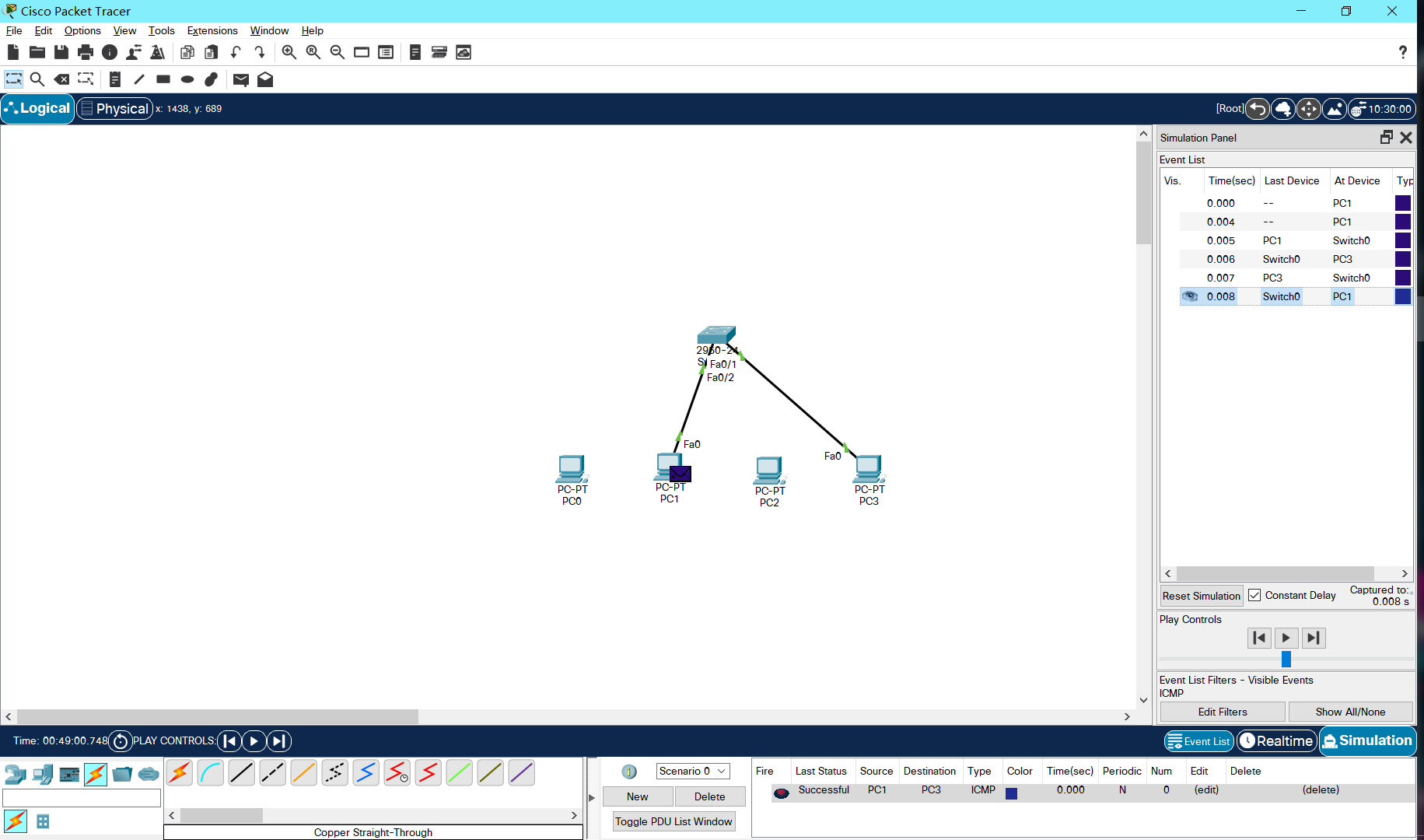
1. 完成交换机端口F0/2安全功能配置；



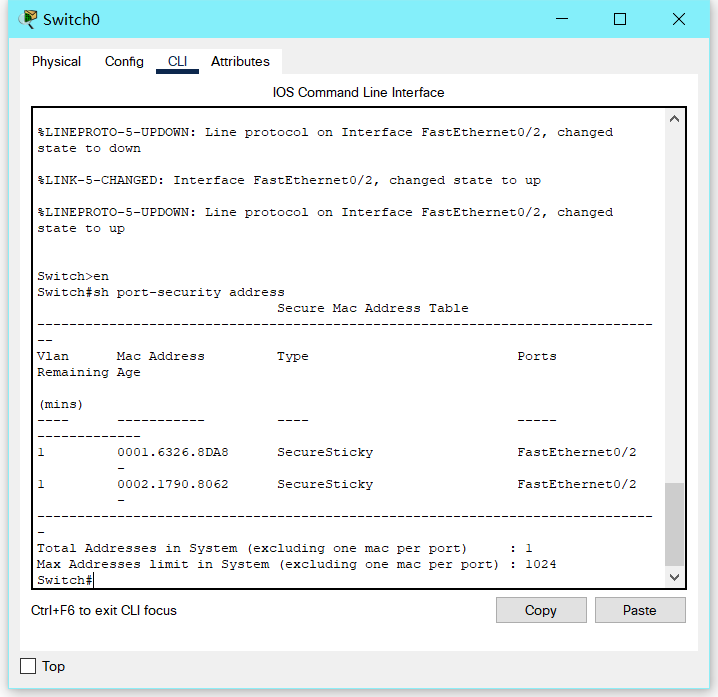
1. 启动PC0与PC3之间的ICMP报文交换；



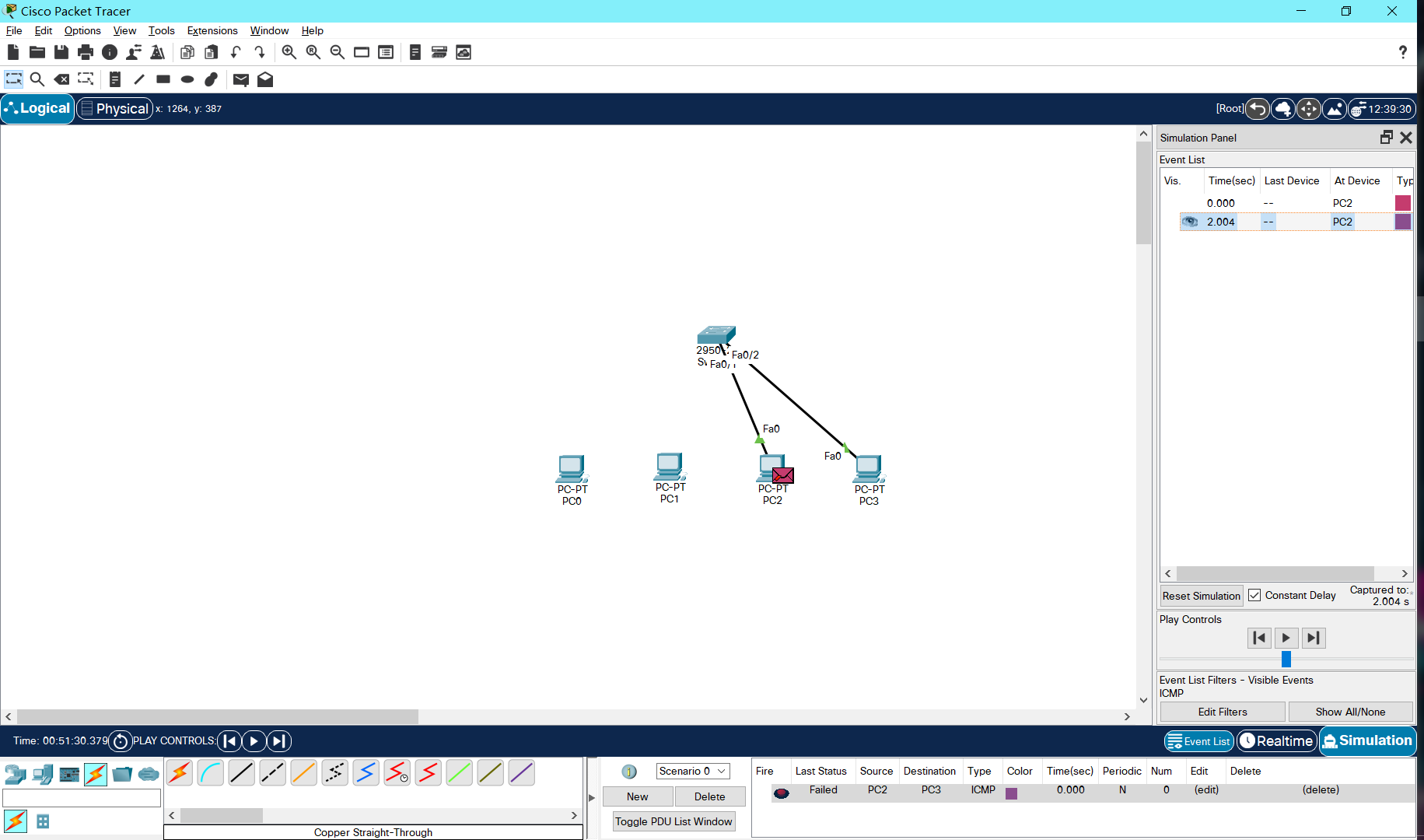
1. 删除PC0与交换机端口F0/2的连接，将PC1连接到交换机端口F0/2，启动PC1与PC3之间的ICMP报文交换；



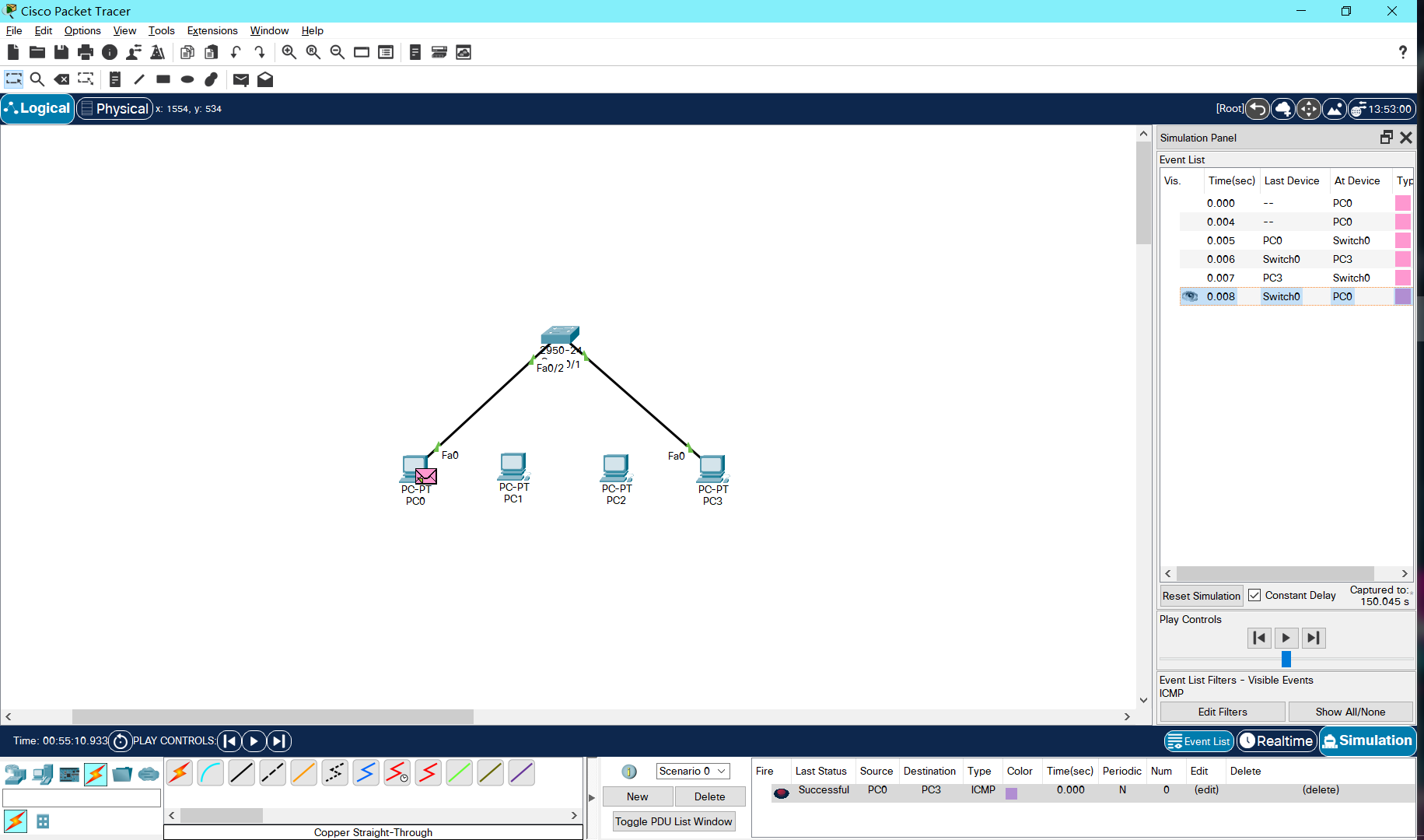
1. 查看访问控制列表中的MAC地址；



1. 删除PC1与交换机端口F0/2的连接，将PC2连接到交换机端口F0/2，启动PC2与PC3之间的ICMP报文交换；



1. 删除PC2与交换机端口F0/2的连接，重新将PC0或PC1连接到交换机端口F0/2，与PC3进行ICMP报文交换。



三、实验结果及分析

配置过网络信息后，PC0、PC1与PC3交换报文以后，访问控制列表中添加了PC0、PC1的MAC地址，由于设置的访问控制列表最大MAC地址数为2，所以此时已经达到最大值。所以PC2启动与PC3交换报文时，MAC地址不属于访问控制列表中的MAC地址，丢弃该MAC帧，PC２无法完成与PC３的ICMP报文交换。重新连接PC０与PC1，来自这两个属于访问列表中的MAC地址的报文，能成功进行交换。

四、实验总结及体会

如果想控制终端的访问，可以在交换机中进行安全功能配置，限制首先交换ICMP报文的终端的MAC地址可以加入访问控制列表，并且设置最大MAC地址数量，这样只要是计划内的终端先进行报文交换，将MAC地址存入访问控制列表并达到最大数量，随后非计划内的终端就无法进行报文交换，MAC帧会被丢弃，达成控制访问的目的。

防DHCP欺骗攻击实验

一、实验目的

(1)验证DHCP服务器配置过程。

(2)验证DNS服务器配置过程。

(3)验证终端用完全合格的域名访问Web服务器的过程。

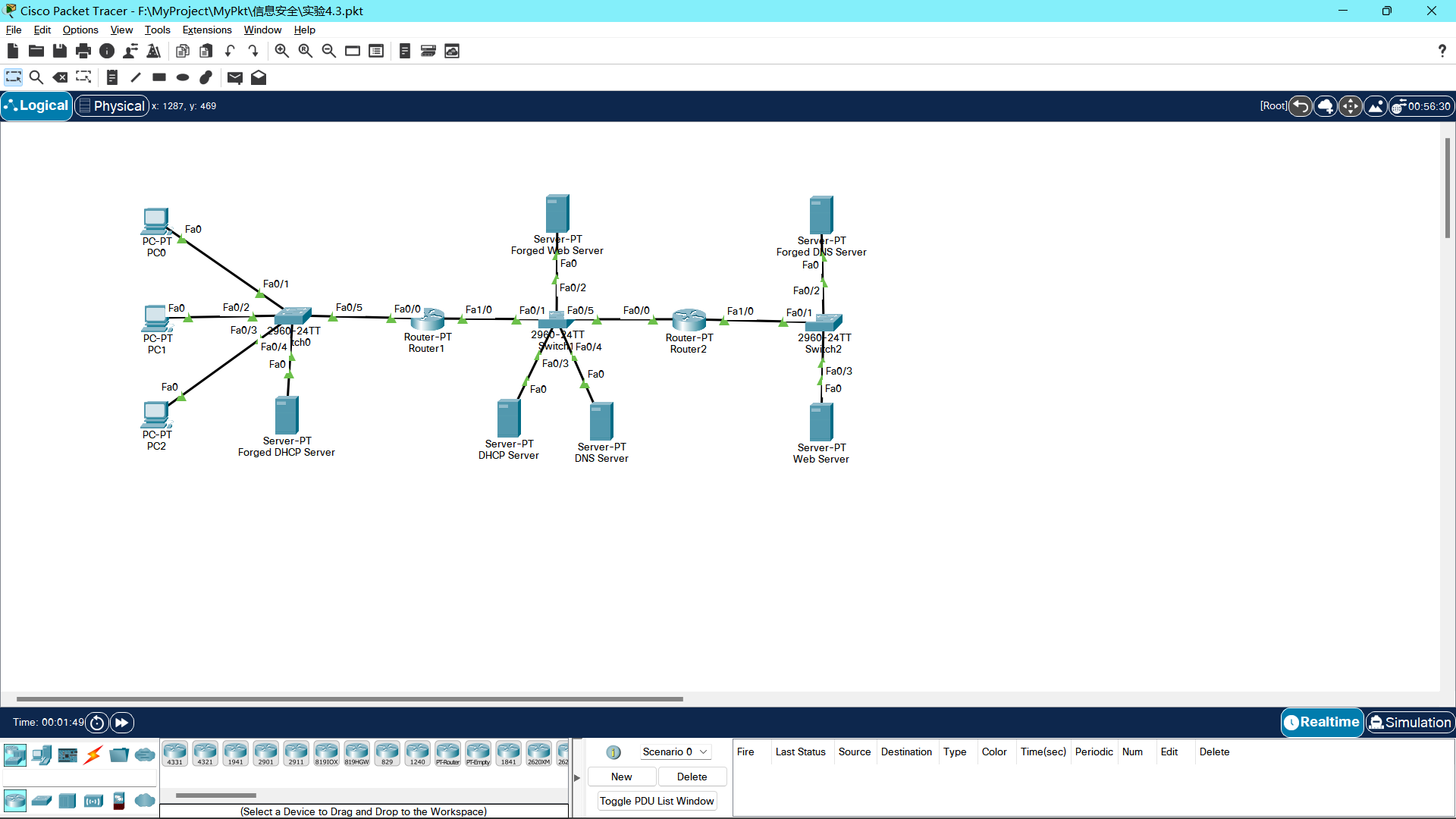
(4)验证DHCP欺骗攻击过程。

(5)验证钓鱼网站实施过程。

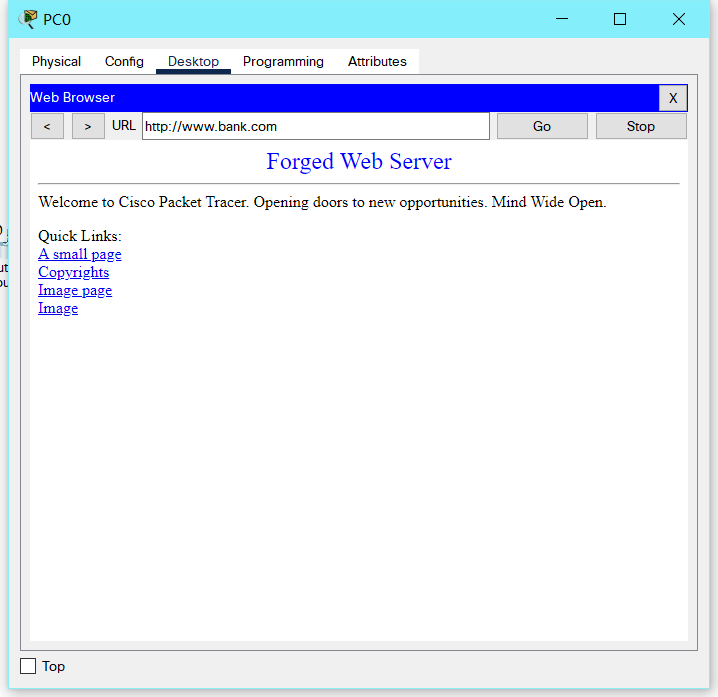
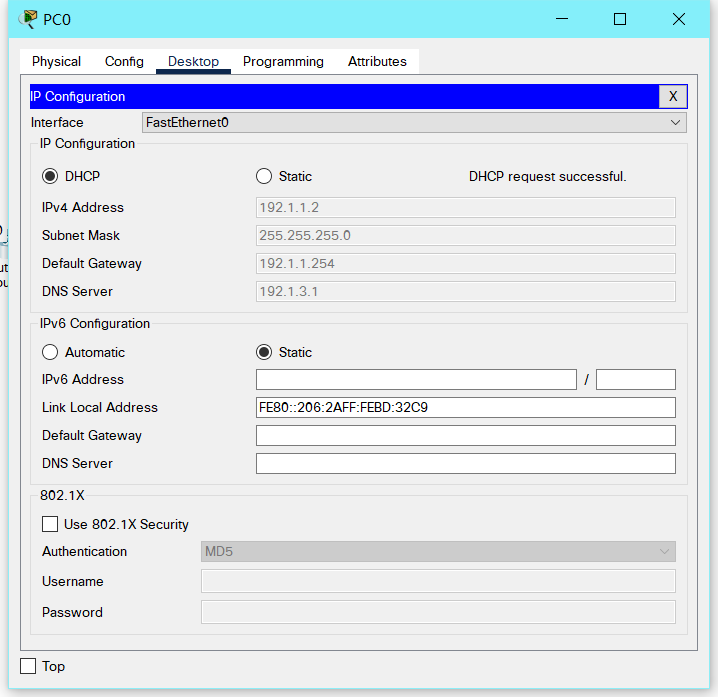
(6)验证交换机防DHCP欺骗攻击功能的配置过程。

二、实验步骤

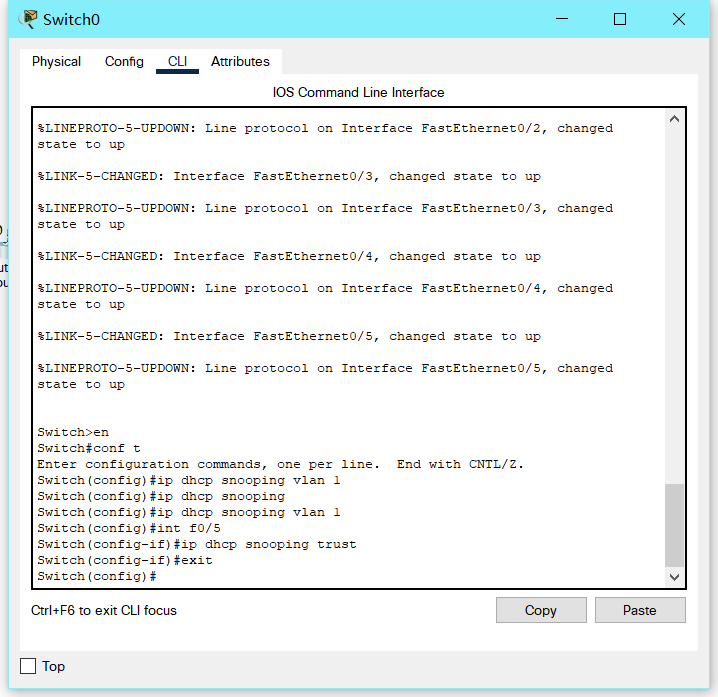
1. 在实验2.5的基础上进行，拓扑图为；



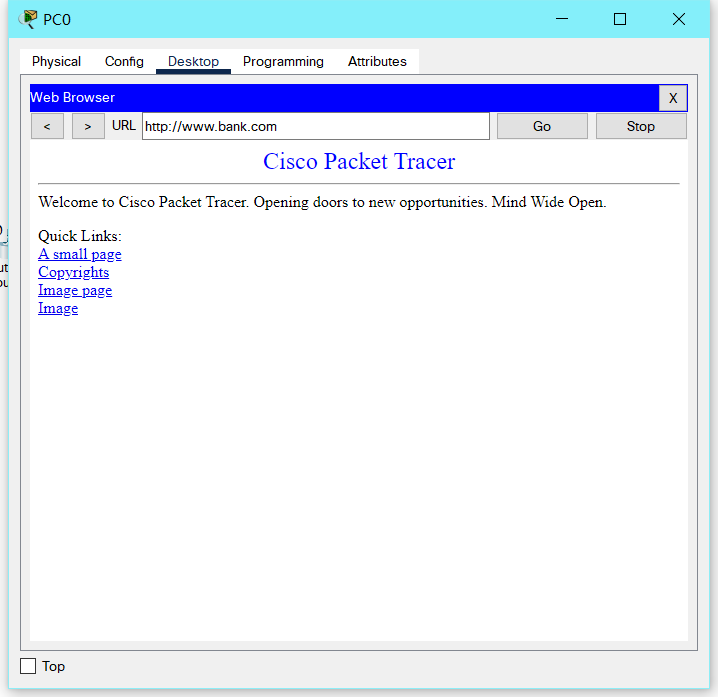
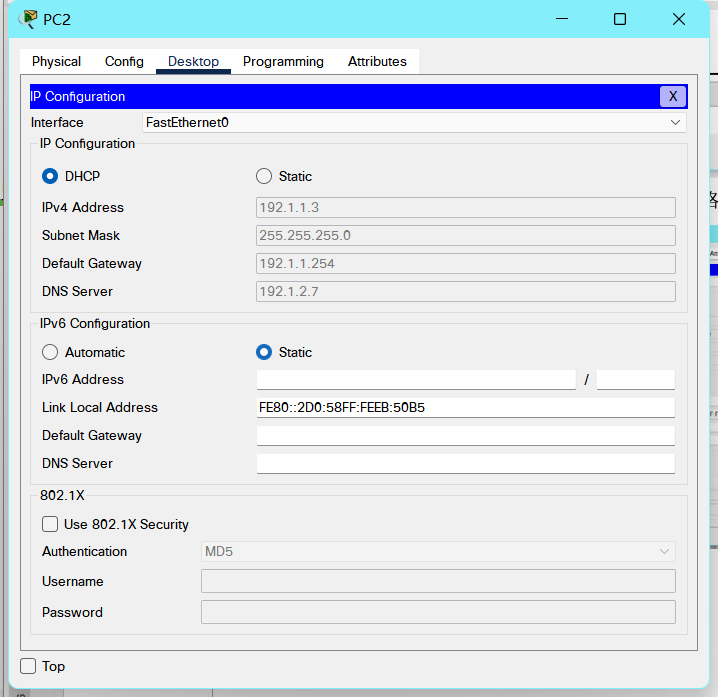
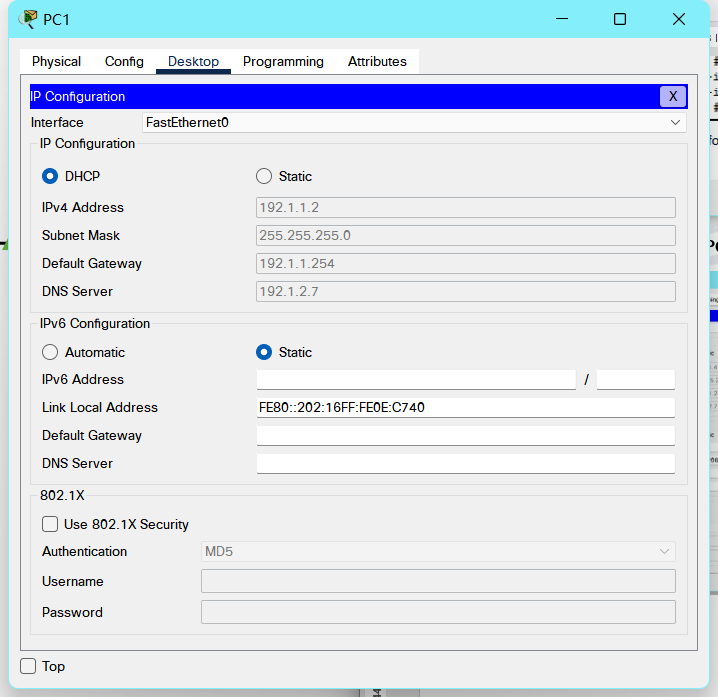
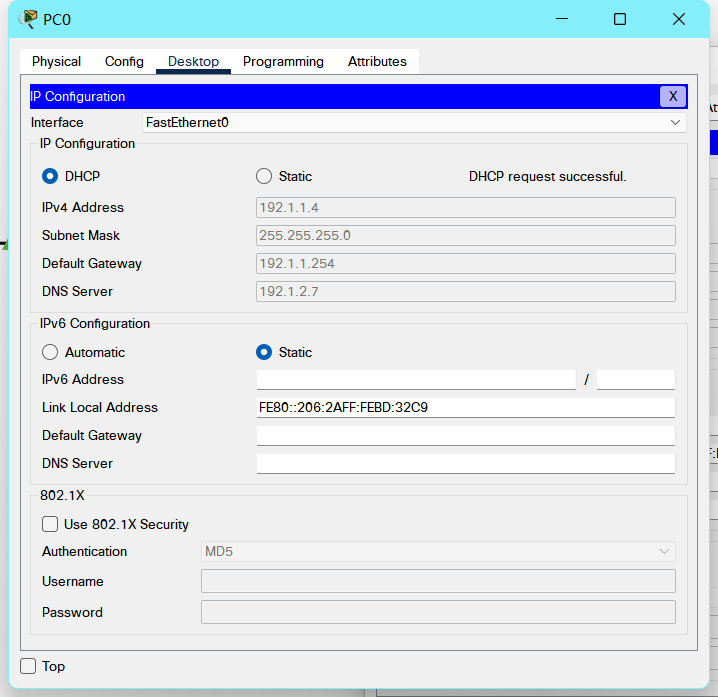
1. 在启动防DHCP欺骗攻击的功能之前，PC0从伪造的DHCP服务器获取网络信息，从而使PC0用完全合格的域名[www.bank.com访问伪造的Web](http://www.bank.com访问伪造的Web)服务器；



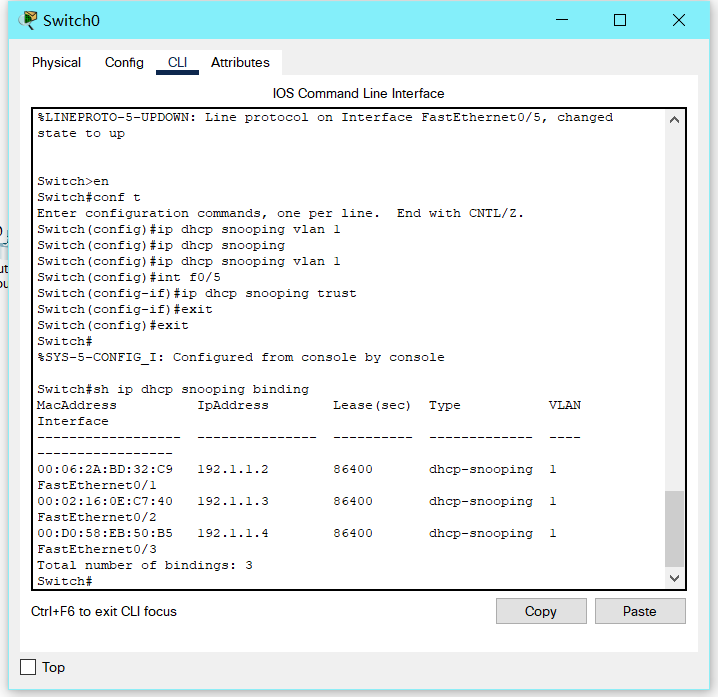
1. 在交换机中启动防DHCP欺骗攻击的功能；



1. 再次让PC0、PC1、PC2通过DHCP自动抓取网络信息，得到的DNS服务器地址为正确的192.1.2.7，通过完全合格的域名[www.bank.com访问正确的Web](http://www.bank.com访问正确的Web)服务器；



1. 查看交换机DHCP帧听信息库的情况；



三、实验结果及分析

实验继用实验2.5，首先让PC0通过DHCP自动抓取网络信息，会得到伪造的DNS服务器地址，从而访问伪造的Web服务器。在交换机中启动防DHCP欺骗攻击功能之后，只有连接在信任端口的DHCP服务器才能为终端提供自动抓取网络信息的服务，PC再通过DHCP自动抓取网络信息就是得到正确的DNS服务器地址，从而访问正确的Web服务器。

实验中将连接路由器R1的交换机端口设置为信任端口，终端只能接收由路由器R１转发的DHCP消息，从而防止了被伪造的DHCP服务器进行欺骗攻击。

四、实验总结及体会

这种防御方法通过限制交换机端口的信任与否来控制终端接收的DHCP消息来源，攻击者只要无法将伪造的DHCP服务器连接在设置信任端口的交换机上，终端就不会接收来自伪造DHCP服务器提供的网络信息，进而保证了用户网络访问的安全性。